Headquarters U.S. Air Force

Integrity - Service - Excellence

Air Force Doctrine Document (AFDD) 2-5, *Information Operations*

Major Marshall Williams

AFDC/DR

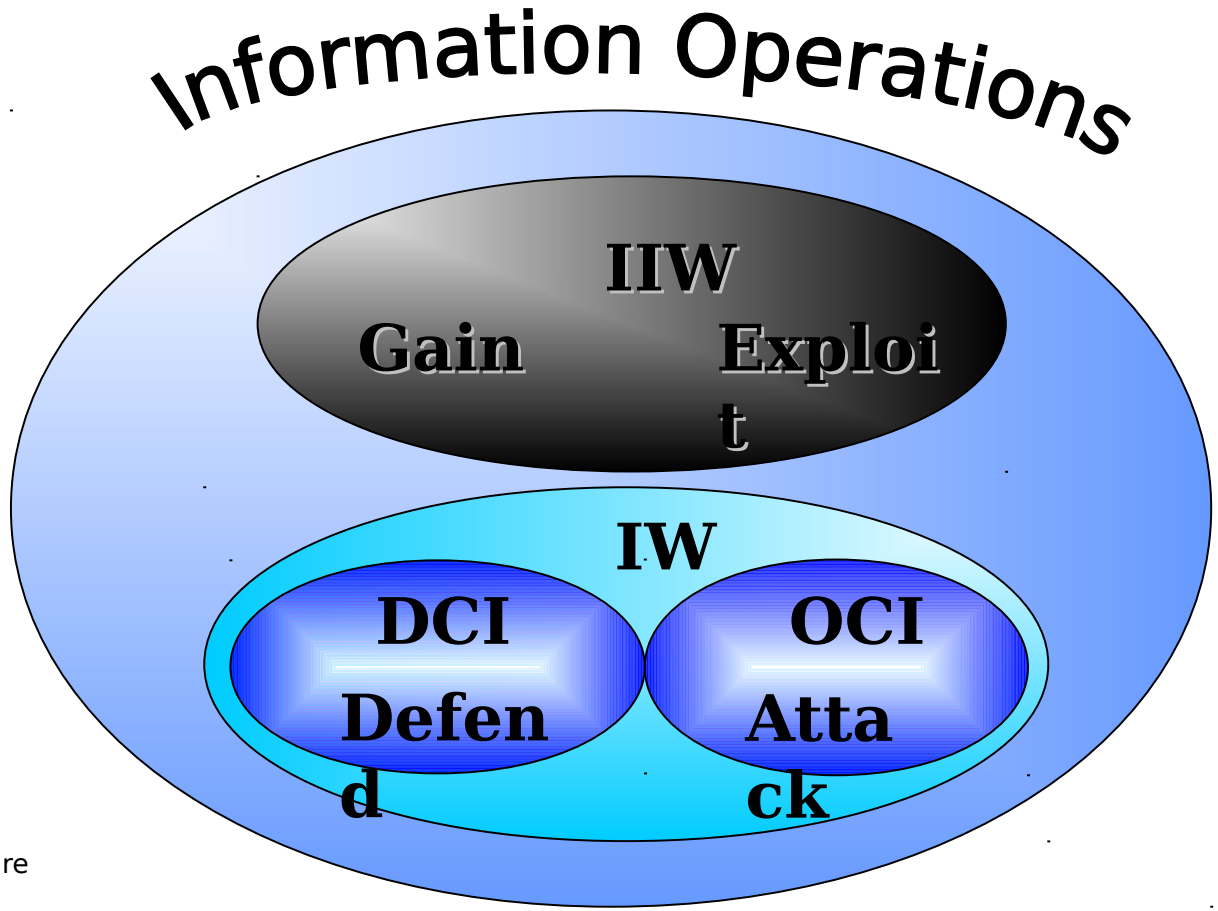
Overview

- CORONA Guidance
- Former Framework
- New Definition and Framework
- IO Military Capabilities
- DoD and Joint Perspectives
- Resolved Key Issues

CORONA Guidance

- **Focus on warfighting – integrate with force application**
- **Focus on the operational level**
  - **Electronic Warfare Operations (Electronic Attack, Electronic Protection, Electronic Support)**
  - **Network Operations (Network Attack, Network Defense, Network Warfare Support)**
  - **Influence Operations (Psychological Operations, Deception, Public Affairs, Counterintelligence, Operations Security)**
- **Incorporate cross-doctrinal concepts – non-kinetic and kinetic options seamlessly integrated**
- **Covers the entire range of military operations**

Former Framework



IW – Information Warfare

IIW – Information-in-warfare

DCI – Defensive counter information

OCI – Offensive counter information

New Definition & Framework

- **New IO definition: "The integrated employment of the capabilities of influence operations, electronic warfare operations, network operations in concert with the specified integrated control enablers, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own."**

Approved by AF Chief of Staff

11 January 2005

Military Capabilities

Influence Ops | Electronic Warfare Ops | Network Warfare Ops

MD | OPSEC | PSYOP | EP | EA | NetD | NetA

Sub-class Capabilities

PA | CI | C-PRO | ES | NS

- **Supported by the Integrated Control Enablers: ISR, Precision Navigation & Timing, Predictive Battlespace Awareness, and Network Operations**
- **Integrated with Physical Attack**

Influence Operations

- **Influence operations focus on affecting the perceptions and behaviors of leaders, groups, or entire populations. Influence operations employ capabilities to affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects across the cognitive domain. These effects should result in differing behavior or a change in the adversary's decision cycle, which aligns with the commander's objectives. The military capabilities of influence operations are psychological operations, military deception, operations security, counterintelligence operations, counterpropaganda operations, and public affairs operations. Public affairs, while a component of influence operations, is predicated on its ability to project truthful information to a variety of audiences.**

Network Warfare Operations

- **Network warfare operations seek to achieve desired effects across the interconnected analog and digital network portion of the battlespace. Networks in this context are defined as any collection of systems transmitting information. Network warfare operations are conducted in the information domain through the combination of hardware, software, data, and human interaction. Examples include radio nets, satellite links, tactical digital information links, telemetry, digital track files, telecommunications, and wireless communications networks and systems. The military capabilities of network warfare operations are network attack, network defense and network warfare support.**

Electronic Warfare Operations

- **Electronic warfare operations use military capabilities to achieve desired effects across the electromagnetic domain in support of operational objectives. Electronic warfare operates across the electromagnetic spectrum, including radio, visible, infrared, microwave, directed energy, and all other frequencies. It is responsible for coordination and deconfliction of all friendly uses of the spectrum (air, land, sea, and space) as well as attacking and denying enemy uses. The military capabilities of electronic warfare operations are electronic attack, electronic protection, and electronic warfare support.**

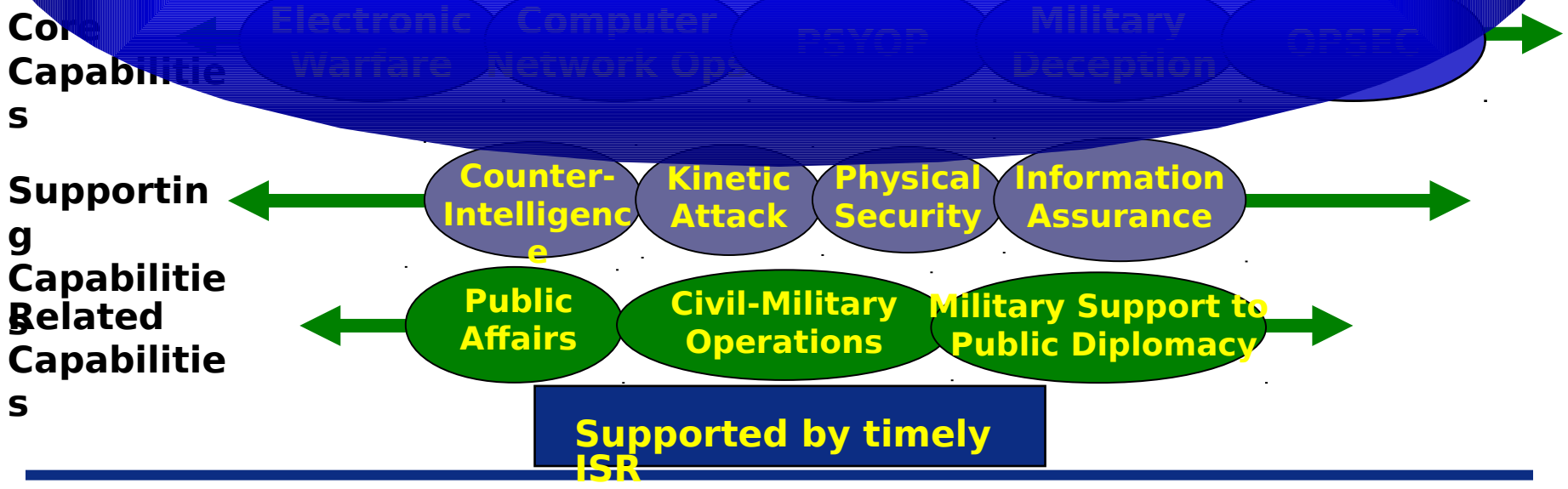
Integrated Control Enablers

- **Integrated control enablers (ICE) are those critical capabilities that support IO, as well as other air and space operations. ICE includes intelligence, surveillance, and reconnaissance (ISR), network operations, predictive battlespace awareness (PBA), and precision navigation and timing (PNT). The seamless integration and interactive relationship of the find, fix, track, target, engage, and assess (F2T2EA) phases continuously provide commanders decision-quality information that is integral to the success of the information operations' attack and defend missions. Because IO are highly dynamic and maneuverable, the transition between the F2T2EA phases can be nearly instantaneous. The ICE components support relationships between gain, exploit, attack, and defend.**

DOD Framework

- **DOD 3600.1 / IO Roadmap definition: "The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own."**

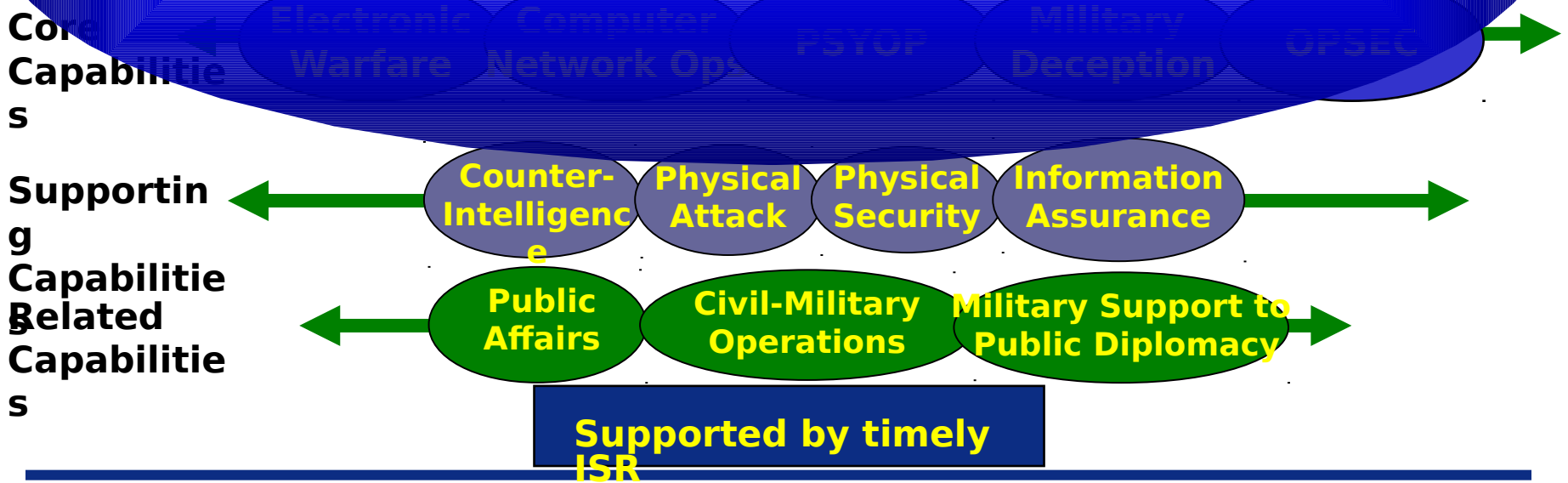
IO Roadmap approved Dec 03; DODD 3600.1 is in abeyance



Draft JP 3-13 Framework

- **JP 3-13: "The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making while protecting our own."**

Second draft currently out



Resolved Key Issues

- Information-in-Warfare
- IO as exclusively nonkinetic
- EW presentation
- IO targeting
- PA presentation
- Role of IO organizations

Information-in-Warfare

- **Issue: Information-in-Warfare included all elements supporting all AF operations (rather than just IO)**
- **Discussion: Explain interactive relationship between the gain, exploit, and disseminate capabilities with those of attack and defend**
- **Solution: Focus on the capabilities providing critical support to IO, and call them “Integrated Control Enablers”**
  - **Integrated Control Enablers (ICE) -- critical capabilities required to execute successful air, space and information operations, provide commanders battlespace awareness, and produce integrated effects for the joint fight**
  - **Includes ISR, PBA, PNT, and NetOps**

IO as Exclusively Non-kinetic

- **Issue: If IO was exclusively non-kinetic:**
  - **Would create a disconnect with DOD framework**
- **Discussion: IO consists of traditionally non-kinetic activities (OPSEC, deception, network defense, etc.), but may have a direct relationship with kinetic activities**
- **Solution: Place verbiage in AFDD 2-5 to reflect scope of IO capabilities**

"Information Operations provide predominantly non-kinetic capabilities to the warfighter. These capabilities can create effects across the entire battlespace and are conducted across the spectrum of conflict from peace to war and back to peace."

EW Presentation

- **Issue: Does EW belong in IO?**
- **Discussion:**
  - **EW is pivotal to all air, space, and information ops**
    - **EW fits many places in doctrine and is represented in *Air Warfare*, *Space Operations*, and IO**
    - **SEAD discussion belongs in both *Air Warfare* and IO**
  - **The future of EW operations is in the IO arena**
    - **Electronic Warfare Operations framework supports this evolution**
- **Solution: Articulate the evolution of EW in IO in AFDD 2-5**
  - **Acknowledge the cross-doctrinal role of traditional EW in air and space warfare**

IO Targeting

- **Issue: Is targeting of IO conducted like air?**
- **Discussion: Need to integrate kinetic and non-kinetic capabilities**
- **Solution: Address targeting in AFDD 2-5 using the following air warfare framework**
  - **Objectives and Guidance**
  - **Development of Desired Effects**
  - **Weaponeering Assessment**
  - **Force Application**
  - **Execution Planning**
  - **Assessment**

Role of IO Organizations

- **Issue: Have we captured the role of IO organizations in support of the JFACC, including reachback, in peace and war?**
- **Discussion: Need to better understand how various IO organizations support the warfighter**
- **Solution: Discuss IO organizations in AFDD 2-5**
  - **Information Warfare Flight (IWF)**
  - **Electronic Warfare Coordination Cell (joint)**
  - **Network Operations and Security Center (NOSC) and Network Control Centers (NCC)**

PA Presentation

- **Issue: Does PA belong in influence operations?**
- **Discussion: PA is a key contributor to IO**
  - **PSYOP, deception, and OPSEC should be coordinated with PA to communicate military intent and avert information fratricide**
  - **Concern is public perception of linking PA to PSYOP and deception activities and presenting PA as an “influence” operation**
    - **The success and legitimacy of PA is predicated on public trust**
- **Solution: PA is an activity of influence ops**
  - **Specific wording in AFDD 2-5 reflects the need to integrate PA in IO while maintaining ground truth and ensuring the necessary separation of PA activities**

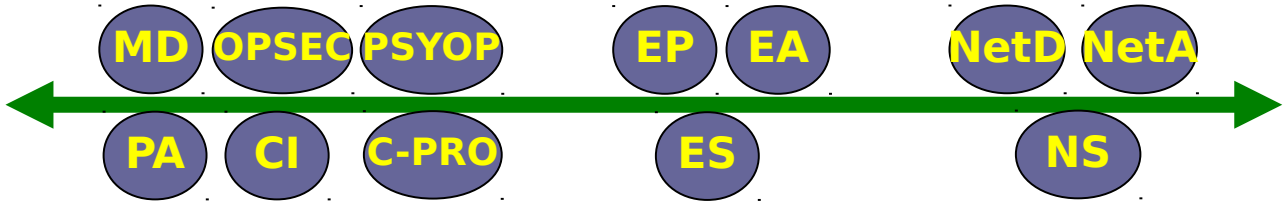
- **AFDD 2-5 available for download from the AFDC website:**

https://www.doctrine.af.mil/

(Note: website restricted to .mil and .gov)

Glossary of Acronyms

Sub-class capabilities



MD – Military Deception

OPSEC – Operations Security

PSYOP – Psychological Ops

PA – Public Affairs

CI – Counterintelligence

C-Pro – Counter

EP - Electronic Protect

EA – Electronic Attack

ES – Electronic Support

NetD – Network Defense

NetA – Network Attack

NS – Network Warfare Support